GENERAL GOVERNMENT

EMERGENCY PREPAREDNESS

Overview

When an individual is confronted by a personal emergency in the United States, he or she can be confident that any 911 call for assistance will be answered promptly, and that a competent authority will respond rapidly. Y2K presents two essential threats to our emergency service and disaster preparedness agencies. First, it threatens to interrupt the ability to properly process and respond to calls for assistance. This threat is present at all levels, from the potential interruption to a citizen's call for fire or police assistance to delays in a state's ability to request emergency or disaster assistance from the federal government. Second, due to lack of experience with anything like the possible affects of the disruptions we may face, it presents a novel challenge to those who must devise Y2K emergency response strategies unlike those they have formulated in the past.

> ***"THERE ARE THINGS THAT CAN SPAWN PANIC AND PANIC DOESN'T HELP PREPARATION. WE NEED TO PREPARE, NOT PANIC."***
>
> ***SENATOR GORDON SMITH***

Most 911 emergency dispatch centers, known as Public Safety Answering Points (PSAP), are highly automated, particularly in the case of enhanced 911 systems. Enhanced 911 systems are those which automatically provide the caller's location and phone number to the 911 operator. According to the FCC, the Association of Public Safety Communications Officials (APCO) has identified 50 pieces of equipment within a PSAP that have Y2K vulnerabilities. There are approximately 4,500 PSAPs located throughout the United States.

Modern emergency dispatch facilities often incorporate sophisticated Computer-Aided Dispatch (CAD) systems into their operations. CAD systems provide important benefits to public safety communication systems, including:

- improved call-taking service to the public,
- provision of greater accuracy, efficiency, and speed in responding to calls for service,
- enhanced officer safety by providing detailed information on call locations, and
- increased officer productivity and resource management and provision of additional system capacity due to growth or crisis.

CAD systems are especially vulnerable to Year 2000 problems due to the fact that they perform time and date calculations on the time an initial call for assistance was received, when a unit was dispatched, the time that it arrived and how long it took to resolve the emergency. These systems are in widespread use in all areas of local emergency service, including police, fire and emergency medical services (EMS).

Sophisticated information technology systems serve as important tools for emergency service agencies today, particularly for law enforcement. Systems such as the National Crime Information Center (NCIC), the National Law Enforcement Telecommunications System (NLETS), Automated Fingerprint Identification Systems (AFIS) and individual criminal information data systems operated individually by all 50 states enable officers to obtain the most up-to-date information on wanted persons, stolen vehicles, criminal histories, and department of motor vehicle records. The ability to access this information dependably and quickly is essential both to officer safety and to the speedy and effective administration of justice at all levels. A recent survey conducted on the effectiveness of NCIC indicates that during a one year period, 81,750 wanted persons were found, 113,293 individuals were arrested, 39,268 missing juveniles and 8,549 missing adults were located and 110,681 stolen cars valued at over $570 million were recovered as a result of NCIC's use.

The Federal Bureau of Investigation (FBI) is responsible for the administration of NCIC and has assured the Committee staff that this system will fully meet its Year 2000 challenge, successfully maintaining its links to the systems of all 50 states. The challenge for local law enforcement agencies is to be sure that their own links to NCIC and NLETS via state maintained connections and any other similar systems operated on a regional or agency-wide level are compliant and compatible with the larger systems. Also, at the local agency level, there often is a great deal of "interconnectivity" between the emergency service department's systems and those of other city agencies, such as the court system, the corrections department, and even local utility companies, thereby increasing the potential for Y2K-related problems in this area.

As is true in other areas, Y2K's presence is insidious in the area of emergency services. One major police department related to the Committee staff that its city's government was required to remediate its gasoline pumps in order to ensure that gasoline would continue to flow to its patrol cars on January 1, 2000. This problem had the potential to affect the entire fleet of city government-owned vehicles. In this particular case, the computerized gasoline pumps perform a time and date calculation based upon the last time a particular gas credit card was used to fuel a vehicle and therefore the pumps were Y2K vulnerable.

In another case, the sheriff of a large western county related that his department was currently examining its computerized detention files which track in and out time of inmates at the county jail facility and hearing date information for inmates. Additionally, a consultant specializing in Y2K public safety problems provided the Committee staff with a list of over 35 items of technical equipment commonly used in law enforcement that could potentially be vulnerable to embedded chip problems. These items included patrol car mounted video equipment, mobile data systems and electronic prisoner monitoring devices used in home detention and probation.

In addition to the technical aspect of Y2K vulnerabilities, emergency service departments must also consider the possibility that January 1, 2000, may bring with it an enormous increase in the demand for their services, depending on the degree of disruption experienced. This must be considered as part of Year 2000 emergency planning at the state, county, and local levels of government.

U.S. Emergency Services Structure

The U.S. emergency service and disaster response sector is a multi-layered safety net consisting of local, county, and state police departments, local and county fire departments, emergency medical service agencies, local, county, and state emergency management organizations, volunteer organizations and a coordinated network of federal resources available when state and local resources are exhausted or overrun. The Y2K problem bears the potential to affect all layers and sections of this safety net. In the event of serious Y2K-related disruptions, many of the organizations that comprise the safety net will be called upon to respond.

According to the Bureau of Justice Statistics, there are over 17,000 police and sheriffs departments in the U.S. The International Association of Fire Chiefs estimates that there are 32,000 fire departments in this country. Additionally, approximately 65 % of our country's EMS agencies reside within the organizational structure of our nation's fire departments.

Statistics provided by the National Emergency Number Association indicate that over 300,000 911 emergency calls are placed in this country daily. (Approximately 110 million calls for emergency assistance per year). An additional 83,000 calls for emergency assistance are placed via cellular phones. Ninety percent of the U.S. population is covered by 911 service.

Each of the 50 states and U.S. territories encompass an emergency management department headed by a state emergency manager. The governors in each respective state appoint many of these managers. The emergency manager serves as the chief disaster preparedness and

response coordinator in the state. Twenty-four states and one U.S. territory are currently signatories to the Emergency Management Assistance Compact. The Compact provides for mutual assistance between the states in managing any disaster or emergency that is duly declared by the governor of the affected state, whether arising from natural disaster, technological hazard, man-made disaster, resource shortages, community disorders, insurgency or enemy attack. This compact also provides for mutual cooperation in emergency-related exercises, testing, or other training activities. While on its face it would appear that this compact would hold the promise of being well-suited to address the many problems that may arise from the Year 2000 problem, discussions with a number of emergency managers reveals otherwise. During her testimony before the Committee on October 2, 1998, Ms. Ellen Gordon, President of the National Emergency Managers Association (NEMA), explained that mutual aid between the states might not be possible in the event that all states are affected in a significant manner.

Individual states might not be able to spare limited resources or be in a position to lend other mutual aid. One state emergency manager told Committee staff that he would be hesitant to release any of his own resources to another state because of the degree of uncertainty about potential Y2K disruptions.

The Federal Emergency Management Agency (FEMA) was established in June 1979 by President Carter to improve the responsiveness of the federal government to catastrophes in the United States. FEMA provides financial and technical assistance to states and localities overwhelmed by disasters. FEMA administers policies related to emergency management and planning, evacuation, and matters associated with civil defense, disaster relief, fire prevention, earthquake hazard reduction, emergency broadcasting services, flood insurance, mitigation programs and dam safety. The principal federal authority for the provision of disaster relief is the Robert T. Stafford Disaster Relief and Emergency Assistance Act (the Stafford Act). The act authorizes the President to issue major disaster or emergency declarations, sets out eligibility criteria and specifies the types of assistance the President may authorize. Aid is provided to meet urgent housing needs, purchase necessary personal items and obtain legal services needed as a result of disasters. Aid is provided to state and local governments and non-profit organizations to repair or reconstruct damaged or destroyed infrastructure, remove debris and to construct protective measures. In addition to the assistance provided by the Stafford Act, federal disaster assistance is also provided by other federal agencies (see description of the Federal Plan).

The Federal Response Plan[1]

The Federal Response Plan (the Stafford Act) established the authority for the federal government to respond to disasters and emergencies in order to provide assistance to save lives and protect public health, safety, and property. It is applicable to natural disasters such as earthquakes, hurricanes, typhoons, tornadoes and volcanic eruptions; technological emergencies involving radiological or hazardous material releases; and other incidents requiring federal assistance.

The Plan establishes the architecture for a systematic, coordinated and effective federal response to disasters or other emergencies. It concentrates the provision of federal assistance a state is most likely to need under 12 Emergency Support Functions (ESF). Each ESF is headed by a primary agency, which has been selected based on its authorities, resources, and capabilities. The 12 ESFs are the primary mechanism through which federal response assistance is provided to the affected state.

Emergency Support Functions

ESF #1 - **Transportation:** U.S. Department of Transportation

ESF #2 - **Communication:** U.S. National Communications System

ESF #3 **- Public Works and Engineering:** U.S. Department of Defense

ESF #4 - **Firefighting:** U.S. Department of Agriculture

ESF #5 - **Information and Planning:** FEMA

ESF #6 - **Mass Care:** American Red Cross

ESF #7 - **Resource Support:** General Services Administration

ESF #8 - **Health and Medical Services:** U.S. Department of Health Human Services

ESF #9 - **Urban Search and Rescue :** U.S. Department of Defense

ESF #10 - **Hazardous Materials:** Environmental Protection Agency

ESF #11 - **Food:** U.S. Department of Agriculture

ESF #12 - **Energy: U.S.** Department of Energy

The Plan describes federal actions to be taken in providing immediate response assistance to one or more

[1]Public Law 93-288 was amended by Public Law 100-707 and retitled as the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law 93-288, as amended).

affected states.[2] Response assistance includes those actions and activities which support state and local government efforts to save lives, protect public health and safety, and protect property. In some instances, a disaster or emergency may result in a situation that affects the national security of the United States. In those instances, other national security authorities and procedures could be used.

Each state has general responsibility for law enforcement, using local and state resources, including the National Guard. In some cases, a state government may experience a law enforcement emergency (including one in connection with a disaster or emergency) in which it is unable to adequately respond. For example, it may be an uncommon situation that requires law enforcement assistance, one that is or threatens to become of serious or epidemic (large-scale) proportions, and one in which state and local resources are inadequate to protect lives and property of citizens or to enforce the criminal law. In the event such a law enforcement emergency exists throughout a state or part of a state (on behalf of itself or a local unit of government), the governor may, in accordance with the Federal Response Plan, request emergency federal law enforcement assistance from the U.S. Attorney General. If the request is approved, federal law enforcement assistance may be provided to include equipment, training, intelligence or personnel.

Our national security is dependent upon our ability to assure continuity of government, at every level, in any national security emergency situation that might confront the nation. Executive Order 12656, the Assignment of Emergency Preparedness Responsibilities, broadly outlines the role of FEMA's director and the National Security Council in response to national security emergencies. Executive Order 12656 defines a national security emergency as **"**any occurrence, including natural disaster, military attack, technological emergency or other emergency, that seriously degrades or seriously threatens the national security of the United States." It establishes the role of the President in national security emergency preparedness. Pursuant to the President's direction, the National Security Council is responsible for developing and administering our national security policy.

Our national security policy dictates that all national security emergency preparedness activities shall be consistent with the Constitution and laws of the United States and with preservation of the constitutional government of the United States.

Effective national security emergency preparedness planning re-

[2] Under the Plan, a State means any State of the United States, the District of Columbia, Puerto Rico, Virgin Islands, Guam, American Samoa, Trust Territory of the Pacific Islands, Commonwealth of the Northern Mariana Islands, Federated States of Micronesia, or Republic of the Marshall Islands.

quires identification of the functions that would have to be performed during such an emergency, development of plans for performing these functions and development of the capability to execute those plans.

Executive Order 12656 establishes that the director of FEMA shall serve as an adviser to the National Security Council on issues of national security emergency preparedness, including mobilization preparedness, civil defense, continuity of government, technological disasters, and other issues, as appropriate. It also states that the director of FEMA also shall assist in the implementation of national security emergency preparedness policy by coordinating with the other federal departments and agencies and with state and local governments, and by providing periodic reports to the National Security Council.

The public has voiced its concern to the Committee regarding the role that the federal government will play in responding to Y2K-related emergencies. Numerous misguided rumors and outright falsehoods are being circulated in some quarters on the Internet about the possibility that "martial law" will somehow be declared by the federal government in response to Y2K emergencies. These rumors and falsehoods will serve only to incite unwarranted public panic and to needlessly heighten public fear and misunderstanding about the Y2K problem. Such irresponsible and reckless speculation has no basis in fact, and it disregards the long history of our nation's commitment to democracy and our own constitutional system of government, which is grounded in the rule of law.

As the aforementioned information illustrates, a well coordinated, pre-existing network exists through which appropriate emergency or disaster assistance may be rendered from the federal government down through the states and local governments when the states request such assistance. Such assistance is rendered within the context of existing legal authority, and in accordance with pre-existing structures as previously described. The Committee strongly believes the emergency and disaster response structures as described within this report to be the appropriate mechanism through which any necessary federal response to Y2K-related disruptions would be provided.

Major Initiatives

On October 2, 1998, the Committee held a hearing to assess the Year 2000 readiness of government at the federal, state, and local level to continue to provide without interruption vital emergency services, such as police, fire and emergency medical services. The Committee also inquired into the ability of emergency response personnel to respond to potential Year 2000-related disruptions, such as interruptions or anomalies in the utility, communications and transportation sectors.

The hearing examined the role of FEMA in coordinating the execu-

tion of the Federal Response Plan, and the role the Plan could play in mounting a federal response to potential Y2K-related interruptions. Also, it explored the extent to which FEMA has considered potential Year 2000 disruptions as events that might require a coordinated federal response.

The hearing examined the state of FEMA's readiness to carry out its mandate under the Stafford Act in light of the Year 2000 problem and focused on FEMA's outreach to the state emergency preparedness agencies and non-governmental organizations that help respond to disasters.

Lacy Suiter, Executive Associate Director of FEMA's Response and Recovery Directorate, provided testimony about the state of FEMA's internal Y2K preparedness, its outreach to state and local emergency management and emergency services agencies, and FEMA's plans to coordinate the federal response to Y2K-induced emergencies.

FEMA's other Y2K initiatives, as described both in Mr. Suiter's written statement and testimony before this Committee are summarized as follows:

- FEMA is working with other agencies in the emergency services sector to develop an outreach plan that will include meetings on Y2K convened by federal agencies, outside meetings that federal officials will attend to increase Y2K awareness, and other communications on Y2K such as letters, public notices, web site information, and brochures. FEMA plans to post this information on its web page.

- The United States Fire Administration, which reports to FEMA, has initiated a multi-phased plan to raise awareness and assess readiness on the Y2K technology problem. The Fire Administration staff issued a suggested article for the fire and emergency services publications on Y2K preparedness, and FEMA has developed a list of frequently asked questions about Y2K in a Y2K brochure. FEMA has distributed the brochure to participants in the National Fire Academy, major fire service organizations, and state fire marshals. FEMA is in the process of conducting a direct mailing of the brochure to approximately 32,000 individual fire departments nationwide. FEMA has also distributed materials to associations of fire and emergency service equipment manufacturers and distributors requesting information on actions their members are taking to ensure that their products are Y2K compliant.

- FEMA is pursuing outreach activities with state and local governments through the National Emergency Management Association (NEMA) and the International Association of Emergency Managers (IAEM). The focus has

been to heighten awareness of state and local government about the seriousness of the problem and to provide Y2K emergency preparedness guidance and information.

- NEMA has identified Y2K as a priority area and has initiated a Y2K dialogue with its members. NEMA has assigned its Preparedness, Training, and Exercises Committee to review and coordinate efforts with FEMA. FEMA is working in partnership with NEMA, IAEM and other organizations to develop preparedness guidance for the entire emergency preparedness community.

- FEMA's regional directors have been asked to contact the state emergency management directors in their region to reinforce the importance of preparedness and compliance at the state level, to emphasize the necessity of state outreach to local governments, and to help identify areas where additional assistance is needed.

- FEMA's Emergency Management Institute has incorporated a "Y2K Show-of-Hands Survey" to gauge the level of Y2K awareness of its participants.

- In November 1998, FEMA's associate director for preparedness, training, and exercises addressed the IAEM 46th Annual Conference in Norfolk, Virginia, to urge local emergency managers to participate in Y2K preparedness activities.

- FEMA is in the process of planning a series of regional "table-top" exercises to ascertain the needs of the states resulting from a Y2K-related emergency.

- FEMA will coordinate a nationwide "table top" exercise some time in the spring of 1999 to conduct an operational simulation of its response to a Y2K emergency.

- FEMA is hosting monthly meetings with primary Federal Response Plan agencies to monitor progress on the Y2K compliance status of the 12 emergency support functions.

- FEMA is developing a "Y2K Supplement" to the Federal Response Plan based on input from the Federal Response Plan agencies and their regional counterparts. Assessments from the emergency services sector and the President's Council on Y2K conversion will influence the composition of the supplement. FEMA plans to publish the supplement by July 1, 1999. The supplement will include a basic plan and annexes for each of the emergency support functions.

Beginning in July 1998, the Committee staff began discussions with FEMA to determine what authority the federal government would have to act in case of serious Y2K disrup-

tions, and how FEMA specifically plans to respond in the event that such disruptions do occur. In his testimony, Mr. Suiter emphasized that FEMA programs represent a "bottoms up" approach in which federal response comes "by invitation only," upon a specific request from the governor of an individual state, in response to specific and identifiable emergencies and disasters. This response is requested by and coordinated through the governor, and never independently by the federal government. This fact is in stark contrast to some of the reckless assertions appearing on the Internet, claiming that Y2K events would serve as an "excuse" for a massive marshaling of federal forces or the suspension of civil legal authority to deal with possible disruptions.

Sufficient legal authority currently exists under the Stafford Act to allow federal resources to be utilized in response to a Y2K-related disruption if, upon application from a state's governor, an "emergency declaration" is made by the President of the United States. While FEMA has no authority to respond to the causes of Y2K disruptions or to provide technical assistance for "Y2K fixes," it can respond to the physical consequences of Y2K disruptions if they constitute a threat to lives, property, public health and safety pursuant to the President's "emergency declaration."

Although FEMA cannot respond to requests for technology support, it could use the federal response system to provide a backup network to ensure that requests for such aid from state and local governments are channeled to the appropriate public/private coordination entities established by the President's Council on Y2K Conversion. FEMA currently has no plans to pre-position resources prior to January 1, 2000, but will activate the interagency Emergency Support Team at FEMA headquarters and its 10 interagency Regional Operations Centers, beginning on December 29, 1999, and continuing through January 4, 2000. FEMA will also place on alert its Emergency Response Support Detachments during that time.

Other Y2k Emergency Services Initiatives

During the summer of 1998, Federal Communications Commission Commissioner Michael Powell began playing a very active role in promoting awareness about potential Y2K-related communications problems in the public safety community. Commissioner Powell authored an article entitled "Protecting Public Safety Communications from the Year 2000 Bug," which was published in the bulletin of the Association of Public Safety Communications Officers International. In June, the FCC held a public safety roundtable which attracted many experts in the field of public safety communications. During the International Association of Chiefs of Police (IACP) Conference held in Salt Lake City October 17-22, 1998, John Clark, FCC deputy chief for public safety in the Wireless Telecommunications Bureau, ad-

dressed the major city police chiefs on Y2K issues. On November 16, 1998, the FCC sponsored a forum entitled "Year 2000: Maintaining Emergency Response Communications." The goal of the forum was to examine the implications of the Y2K problem for various segments of the emergency response communications system.

The State of Texas sponsored a 2-day national conference on October 15 and 16, 1998, for correctional facilities, law enforcement, and emergency services on the topic of the Year 2000 and embedded systems.

In his written statement to the Committee, Sergeant John Powell, University of California Police Department, Berkeley, California, detailed several initiatives that the Association of Public Safety Communications Officials International (APCO) and the IACP are conducting on Y2K.

Sergeant Powell reported that APCO and the National Institute of Justice were discussing the development of a series of short Y2K seminars targeted at public safety chief officers and upper-level management to address four key Y2K impact areas. These areas are internal systems; potential disruption of outside services such as power, 911 service, and supply chain interruptions; the additional workload that could confront agencies due to heightened fears about the problem and the advent of the actual problem itself; and the special needs of agency employees during the time of impact.

During its August 1998 conference in Albuquerque, New Mexico, APCO conducted Y2K seminars to address the broad array of issues confronting public safety agencies. The IACP Communications and Technology Committee included Y2K on its agenda at the IACP conference this year.

First Alert System

In preparing for the October 2, 1998 Hearing on General Government/Emergency Services, the Committee staff formulated the concept of a Year 2000 problem early-warning system dubbed the "Y2K First Alert." Similar to the National Weather Service's storm warning and monitoring system, the Y2K First Alert would provide American citizens with the earliest possible warning of Y2K events that may threaten public safety or national infrastructure. Senators Bennett, Dodd, and Collins jointly expressed their support for the development of this concept during the opening remarks of the October 2, 1998 hearing.

First Alert would give citizens of the eastern United States up to 17 hours advanced warning of the effects of the Year 2000. Other Americans will have proportionately more warning the farther west they live. For example, citizens in Utah will have up to 19 hours of advanced notice while citizens of Hawaii and some citizens

of Alaska will have almost a full day's notice. This system would be most useful for problems that occur at or very near midnight, December 31, 1999, which could be referred to as Y2K "prompt effects." These effects could occur in embedded systems in utilities, transportation, telecommunications and other applications that had not been repaired. They could also occur in mainframe or information technology systems that serve a control or supervisory role that had not been fixed. When the century change occurs, a Y2K prompt effect may very quickly cause problems that might lead to some disruption of an important service.

The Y2K First Alert concept is feasible because of the arrangement of international time zones. A new day begins in the middle of the Pacific Ocean, 17 time zones earlier than Eastern Standard Time in the United States. If the Y2K bug is potent enough to cause immediate problems or “prompt effects” in information systems and embedded chips, the effect will not occur worldwide all at once. Rather, the problems will happen repeatedly in one time zone after another for one full day. For example, Y2K problems that occur at precisely 12:00 a.m. on January 1, 2000, in Wellington, New Zealand, are occurring while it is still only 7:00 a.m. on December 31, 1999 in the eastern United States. Systems and technology vulnerable to Y2K prompt effects in the eastern United States will not be affected for another 17 hours by the century rollover.

The Committee believes it is imperative to use this advance notice that the United States has for the good of the nation. For instance, it would be very useful to know that utility and transportation problems are likely to occur based on our Y2K First Alert system before large segments of the population are away from their homes celebrating on New Year's Eve. The Committee has called for the government to implement this concept by coordinating the resources of the Departments of State and Defense as well as other departments and federal agencies that have resources and expertise to contribute to the system.

Since the Committee issued its call on October 2, 1998 several parties have acted. FEMA has begun exploring the implementation of the concept. The telecommunications industry has begun developing a similar, private-sector concept named "Follow the Sun," and it now appears that the U.S. Air Force is pursing a related concept to meet its mission needs. Finally, the Canadian government announced in January 1999 that it plans to implement a similar concept.

Assessments

In accordance with the President’s Council on the Year 2000 outreach program, the U.S. Fire Administration has been charged with monitoring the progress of the fire response agencies. Outreach to the law enforcement sector of public safety has been assigned to the Department of

Justice.

While there was a high level of Y2K awareness among the limited number of representatives of individual emergency service agencies contacted by the Committee staff in preparation for the October 2, 1998, hearing, the major emergency service professional associations were just beginning to coordinate Y2K awareness programs. During her opening remarks to the International Association of Chiefs of Police Conference in Salt Lake City, Utah, in October 1998, Attorney General Janet Reno made no mention of Y2K. Some federal agencies that have regular contact with state and local criminal justice agencies were just beginning to promote awareness about the Y2K problem among the state and local agencies. The National Institute of Justice and the Bureau of Justice Assistance reported no specific or focused Y2K initiatives in progress as of the October 2, 1998, hearing. The National Institute of Justice reported that it was in the process of developing a Y2K awareness bulletin, and that it had incorporated a Y2K compliance stipulation into its grant agreements with state and local agencies.

As part of the Justice Department charged with outreach to the law enforcement community under the President's Council, both the National Institute of Justice and the Bureau of Justice Assistance could be playing a more active role in spreading Y2K awareness among state and local law enforcement and other criminal justice agencies. These agencies have a broad range of contact with criminal justice and law enforcement organizations at the state and local level of government and bear the potential to make a positive impact on the Y2K problem in the emergency service sector. As the available survey data indicates, there is a startling lack of preparedness at the state and local levels of government. All efforts to alleviate this problem should be pursued.

Almost all of the command-level emergency service personnel contacted by the Committee staff expressed serious concerns about a perceived lack of Y2k awareness on the part of emergency service agencies in general. To date, there has been no known large scale attempt to gather any meaningful survey data to measure the overall level of awareness or preparedness of this vital sector.

Concerns

While it is clear that an effective mechanism exists at the federal level to coordinate resources in the event of Y2K related emergencies or disruptions, there is still concern about the Y2K awareness and preparedness levels of emergency service providers at the county and local levels. The strong leadership role that FEMA has recently assumed in the area of Y2K emergency preparedness should have a positive impact on the state and local emergency management network and hence on the nation's overall ability

to respond adequately to Y2K-related emergencies. The overall Y2K preparedness status of state and local emergency service agencies remains unknown, as does the extent to which these agencies have considered Y2K as an event for which they must creatively plan.

In his testimony before the Committee, Mr. Bob Cass, city manager of Lubbock, Texas, described the Y2K emergency simulation exercise that Lubbock had conducted just 2 days prior to the date of the Senate hearing. This exercise gained major nationwide media attention and served as an excellent example of the type of emergency planning activity that local, county and state governments should replicate. Bruce Romer, Chief Administrative Officer of Montgomery County, Maryland, also testified about Montgomery County's plans to conduct a similar exercise in December 1998. Mr. Romer has stated to the Committee staff that Montgomery County plans to activate its Emergency Operations Center prior to December 31, 1999, and said that in the event of a Y2K emergency, he "doesn't want to be looking around for people they will need." Both Lubbock, Texas and Montgomery County, Maryland represent model cases of effective Y2K emergency preparation.

In his written statement to the Committee, Sergeant Powell emphasized the difficulty of accommodating the additional demand for emergency services that may accompany the century date change, due in part to the possible increase in public fear toward the end of 1999. Of great concern to the Committee is the need for effective dissemination of credible information to the general public about the expected level of severity of Y2K disruptions. Governments at all levels must work constantly over the next year to obtain accurate information in order to dispel irrational and unwarranted fears about the potential impact of Y2K disruptions.

FEDERAL AGENCIES

Overview

On the whole, federal agencies have been slow out of the gate in the race to cross the finish line for Y2K efforts. In this race, even though one agency or another may at times lead the pack, all agencies must cross the finish line together in a tie. As the race enters the home stretch, agencies must pick up the pace and sense of urgency. Although much progress has been made this year, the home stretch of this course is daunting.

As expected, those that started the earliest generally lead the pack. The Social Security Administration and Small Business Administration are notable agencies in front that started in the late 1980s. Considering the lead these agencies have over those that started in 1996, one can only conclude that late starters face a formidable task. The most notable agencies that have found themselves in that unenviable posi-

tion include the Departments of Energy, Defense, and Health and Human Services.

All federal agencies are addressing the problem via a five-phased process: awareness, assessment, renovation, validation, and implementation. The next milestone occurs in January 1999 when agencies should complete the validation phase. The last milestone, completion of implementation, occurs in March 1999. Due the tremendous scope and pervasiveness of potential Y2K problems, federal agencies have managed the problem through a triage process. They have identified those systems that are 'mission-critical' to their ability to perform core capabilities. This triage process is deceptively complicated due to the interconnectedness of today's systems. The total effort comes down to risk management, mitigation, and avoidance.

Although agencies are focused on mission-critical systems, many other systems are too important to be completely ignored. These systems are being tracked and actively worked on at a lower priority, according to agencies' reports.

Initiatives

General Accounting Office

GAO has developed and published three guides that address the Y2K problem. These guides are available at *www.gao.gov/y2kr.htm*. A short description of each follows:

- The first guide, Year 2000 Computing Crisis: An Assessment Guide, was published in September 1997. This guide walks step-by-step through the five-phase process and provides a program assessment checklist.

- An exposure draft of the Year 2000 Computing Crisis: A Testing Guide was released in June 1998 and was published in November 1998. This guide provides a Y2K testing step-by-step framework. As with the conversion model described in the first guide, the test model consists of five steps: testing infrastructure, software unit testing, software integration testing, system acceptance testing and end-to-end testing.

- The final guide in the series, Year 2000 Computing Crisis: Business Continuity and Contingency Planning, was published in August 1998. This guide recognizes that not all systems will be fully remediated through the five-phase process before there is a Y2K impact. Additionally, as always, the unexpected and unanticipated must be planned for even when systems have completed all five phases of remediation. An excerpt from the guide notes, "Every federal agency must ensure the continuity of its core business processes by identifying, assessing, managing and mitigating its Year 2000 risks. This effort should not be limited to the risks posed by Year 2000-induced failures of internal information systems, but

must include the potential Year 2000 failures of others, including business partners and infrastructure service providers." The structure described in this guide covers four phases: initiation, business impact analysis, contingency planning and testing.

Emergency Supplemental Funding

Included in the Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Public Law 105-277, were provisions for $2.25 billion for non-defense agencies and activities. The Department of Defense received a separate allocation of $1.1 billion. These monies are to remain available until September 30, 2001. The purpose of these funds is to provide for expenses necessary to ensure that the information technology that is used or acquired by the federal government meets the definition of Year 2000 compliant and to meet other criteria for Year 2000 compliance as the head of each department or agency considers appropriate.

At the time this report was written, two submissions for release of emergency supplemental funds for non-defense agencies and activities had been made: November 6, 1998, and December 8, 1998. The total amount identified in these submissions is $1.23 billion, $891 million and $338 million respectively. This accounts for almost 55% of the total emergency funds available for non-defense agencies and activities. The Department of Defense has yet to submit any documentation for release of any of its $1.1 billion emergency funds for Y2K.

House Committee on Government Reform's Subcommittee on Government Management, Information, and Technology and the House Committee on Science's Subcommittee on Technology

During the 104th Congress, the House held the first hearings to review and investigate the federal government's preparedness for Y2K. Its efforts have provided critical oversight and stimulation of agency efforts. To have the broadest impact possible, both Senators Bennett and Dodd consciously narrowed our Committee's primary focus to concentrate on the private sector and those federal agencies that provide a service to crosscutting segments of the private sector. Detailed information on Representatives Horn's and Morella's activities is found at *www.house.gov/reform/gmit/* and *www.house.gov/science/y2k.htm.*

Office of Management and Budget

OMB is responsible for monitoring agency progress and efforts in addressing Y2K. Its strategy to ensure agency Y2K compliance is based on agency accountability. Progress is monitored through agency goals for compliance of mission-critical systems, progress on the status of mission-critical systems, status of mission-critical systems being repaired, and agency Y2K cost estimates. Progress reporting of federal agencies is on a quarterly and/or monthly basis depending on the tier that

the agency is assigned to by OMB. The three-tier system that OMB is using consists of

> **Tier 1** agencies: *NOT making adequate progress,*
>
> **Tier 2** agencies: making *progress, but with concerns,* and
>
> **Tier 3** agencies: making *satisfactory progress*.

Subsequent to agency submission of quarterly status reports to OMB, OMB generates a consolidated report based on agency self-reported information. OMB's 7th Quarterly Report was issued on December 8, 1998. It is based on data as of November 15, 1998.

Efforts by OMB to provide oversight are often augmented by internal audit organizations within agencies and by GAO.

CIO Council Subcommittee on Year 2000

Among the Federal Government's Y2K initiatives, formation of the Chief Information Officers (CIO) Council Subcommittee on Year 2000, formerly the Year 2000 Interagency Committee, is the oldest. The committee was born in November 1995 when it held its first meeting. The Year 2000 Interagency Committee was an informal committee headed by Kathy Adams from the Social Security Administration. The Committee's purpose was to raise Y2K awareness, address crosscutting issues affecting many or all federal departments or agencies, seek mutual solutions where possible and share best practices.

The Information Technology Management Reform Act established a CIO Council to review and provide guidance on crosscutting information technology (IT) issues. During November 1996, the CIO Council designated the Year 2000 Interagency Committee as an official subcommittee and renamed it the CIO Council Subcommittee on Year 2000. The Subcommittee was instrumental in assisting OMB's development of the Y2K quarterly status report.

President's Y2K Conversion Council

Executive Order 13073 established the President's Council on Year 2000 Conversion in February 1998. The Council has the mandate to oversee agencies' activities to assure that their systems operate smoothly through Y2K. It is responsible for coordinating the federal government's Y2K efforts. Representatives from more than 30 major federal executive and regulatory agencies comprise the Council. These executive representatives are sufficiently senior so as to have 1) extensive knowledge of their agencies' Y2K efforts and external organizational relationships and 2) authority to commit their agencies.

The Council has established over 30 sector groups with coordinators from the appropriate federal agencies charged with outreach into the public and private sectors, both do-

mestically and internationally. Looking internally at federal systems, the Council's oversight includes ensuring that adequate financial and personnel resources are committed to federal Y2K efforts and that they are used effectively.

Assessments

Cost estimates continue to be on the rise for federal agencies. Since August, estimates have risen $1 billion to $6.4 billion. Over 80% of the increase is attributable to three departments: Health and Human Services (HHS), Treasury, and Defense. HHS hiked its estimate $165 million for potential contingencies in fiscal year 2000, Treasury increased its estimate by $53 million for increased testing and validation and Defense jumped $591 million for increased independent verification and end-to-end testing. With much testing to go and schedules closer to possible slippage, it is likely that these cost estimates will continue to rise.

Sixty-one percent of federal mission-critical systems are now reported as compliant. This is a 10% increase since August. The remaining 39% is scheduled for completion by March 1999. Unfortunately, slippage is already apparent. Ten percent of mission-critical systems did not reach the renovation milestone of September 1998. As we move further into 1999, the risk of schedule slippage will increase.

Currently, of 24 major agencies that comprise the federal CIO Council, six are in Tier 1, seven in Tier 2 and 11 in Tier 3. Table 1 identifies these agencies by tier. This is based on self-reported progress on mission-critical systems.

Tier	Agencies
One	DOD, DOE, HHS, DOS, DOT and AID
Two	USDA, DOC, Education, DOL, DOJ, Treasury and OPM
Three	DOL, VA, EPA, FEMA, GSA, HUD, NASA, NRC, NSF, SBA and SSA

Table 1: Current Status of Federal Agencies

Concerns

The Committee is very concerned about current agency progress. Despite an apparent increase in activity, it is still not enough. Many schedules show a steep improvement curve just before key OMB milestones. Both internal audit reporting and GAO reporting support the concern over schedule. Furthermore, hearings by the House specifically focused on the federal government's preparedness continue to raise warning flags. The federal government has never received a passing grade on any of the six report cards issued by Congressman Stephen Horn. Additionally, a large portion of testing, known to be one of the largest portions of the overall Y2K effort, is yet to come. Several agencies stand out as ones that require fo-

cused oversight and stepped up efforts due to the risks associated with their current pace of progress: Healthcare Finance Agency (HCFA), Federal Aviation Administration (FAA), Department of Energy (DOE) and Department of Defense (DOD). In light of these risks, these agencies' business continuity and contingency plans become even more important.

The area of system interfaces is another concern that requires additional attention. These interfaces exist internally within each federal agency; they exist between different agencies, between agencies and state governments, and between agencies and local governments. Generally, these interfaces support government revenue collection systems and benefits payment systems. Often, it is not clear who is responsible for interfaces among federal, state and local governments. Furthermore, the testing is complicated by the need to test these interfaces as a portion of the overall testing strategy.

One prime example is HCFA, which is one the farthest behind in its critical systems remediation efforts. HCFA manages Medicare, Medicaid and Child Health programs serving over 74 million Americans. Problems with federal systems combined with Y2K failures state and local government systems, or the interfaces between them, could result in delayed benefit payments, payments not being received at all or delivered to the wrong party, eligible recipients not receiving payments or incorrect amounts disbursed. Given the extreme volume of transactions that occur daily to support these programs, a contingency plan consisting of manual processes would not suffice.

Finally, half of the emergency supplemental funds for non-defense agencies have already been released within the past 2 months. These funds were intended to stretch over a 3-year period, which suggests that little will remain for true emergency requirements. It is not clear that OMB scrutinized funding requests as closely as the Committee would have hoped. While OMB is experienced in overseeing budgetary requests, another entity more involved with the Y2K issue, such as the President's Council, might have been better fit to evaluate the Y2K funding requests. Unfortunately, suggestions from the House to give more authority and responsibility to the President's Council have yet to take root.

DEPARTMENT OF DEFENSE

In addition to the concerns expressed above, the Department of Defense (DOD), as the largest federal agency with nearly half of the federal government's computer assets, faces a monumental management challenge in addressing Y2K. The department relies on computer systems to conduct nearly all of its functions, including strategic and tactical military operations; sophisticated weaponry; intelligence collection, analysis, and dissemina-

tion; security efforts; and more routine business operations such as payroll and logistics.

The breadth of the problem confronting DOD is enormous: it has more than 1.5 million computers, 28,000 automated information systems and 10,000 networks. Its information systems are linked by thousands of interfaces that exchange data within DOD and across organizational and international lines. Furthermore, DOD's reliance on computer systems is increasing as technology changes the traditional concepts of warfighting through improved intelligence and rapidly modernized command and control. Successful defense operations will depend greatly on the department's ability to ensure that its systems and the systems with which they interface are Year 2000 compliant.

According to the U.S. General Accounting Office (GAO), which published a series of reports last year on DOD's overall efforts to address the Year 2000 problem, the department's efforts pose considerable risks. DOD still does not have reliable, timely information on program status, because information being reported up-the-chain is not validated for accuracy or completeness. GAO found instances in which defense components' reports on systems compliance were often inaccurate. In addition, GAO found that guidance issued by the department to its components on issues such as interfaces, testing, and reporting has been inconsistent, leading to false starts and uncoordinated efforts. GAO also found that DOD's contingency plans, developed in the event of systems failures, are frequently not executable.

DOD's Inspector General and other internal audit offices have issued over 130 reports that similarly question the department's management of its Year 2000 program. These audit reports repeatedly revealed many of the same findings as those reported by the GAO, as well as problems experienced in assessing and inventorying systems, effectively determining and allocating resources, and accurately testing and certifying systems' Year 2000 compliance. The department's audit reports also revealed that much of DOD's base level infrastructure, such as security systems, telephone switches, traffic control systems, and water and sewage treatment systems are vulnerable to Year 2000 problems.

These findings and risks are reflected in the Office of Management and Budget's assessment of DOD as a "Tier 1" agency, i.e., an agency showing "insufficient evidence of adequate progress." DOD senior management has been responsive to the GAO and internal audit findings and has taken an active, highly visible interest in implementing corrective actions. The senior management team has improved its oversight of the Year 2000 program so that it can more effectively assess program direction and take actions

based on this assessment and known problems. However, DOD remains behind schedule in completing its systems remediation and is at considerable risk of being unable to successfully meet the Year 2000 deadline.

STATE AND LOCAL GOVERNMENT

Overview

In addition to the 50 state governments, there are 3,068 county government jurisdictions and approximately 87,000 other local government jurisdictions within the United States.

These state, county, and local governments deliver the majority of the essential services upon which citizens rely each day. These include police, fire, and emergency medical services response; financial support networks, including welfare and Medicaid payments; unemployment insurance payment systems; disability claims; and basic utilities, such as water and wastewater, sanitation, and local transportation systems. While the prospect of preparing federal government systems is daunting, the challenge of assuring the Y2K preparedness of these other sectors of government is even more mammoth. The consequences of failures in this sector are as potentially grave to the public as failures in the vital sectors of power and telecommunications.

Initiatives

Several of the largest intergovernmental councils and professional organizations are actively engaged in Y2K awareness programs. The National League of Cities, the National Association of Counties, and the International City/County Management Association, in conjunction with Public Technology, Inc., are sponsoring a Y2K awareness program entitled "Y2K and You." The Metropolitan Washington Council of Governments has published a Year 2000 Best Practice Manual. These programs are good examples of what an effective dialogue between state, county, and local governments can achieve.

In his testimony before the Committee on October 2, 1998, the Honorable Michael O. Leavitt, governor of Utah and vice chairman of the National Governor's Association (NGA), described several NGA initiatives aimed at assisting the states with Y2K preparation. In July 1998, the NGA held a "Year 2000 State Summit" which focused on state, local, and private-sector coordination and on establishing a common agenda to increase public confidence in state services. The NGA has also published an issue brief entitled "What Governors Need to Know About Y2K," which Governor Leavitt stated "outlines the steps governors should take as chief executive officers, guarantors of public safety, and public leaders." Both the State of Texas and the State of Pennsylvania have been recognized as having two of the most extensive and well-developed state Y2K programs. New York State Governor George Pataki has also been leading the

call for Y2K preparedness in his state.

Assessments

The assessments of Y2K progress in the sector of state and local government are not optimistic.

The National Association of State Information Resource Executives (NASIRE) is conducting a continuing survey of individual state Y2K preparedness. The Gartner Group has also conducted a state government Y2K survey. The National Association of Counties (NACO) recently commissioned National Research, Inc. to conduct a random survey of the Y2K status of county governments. The General Accounting Office (GAO) is examining the status of federal to state data exchanges. These include the vital connections through which funding from the federal government is provided to the states for various aid programs.

Unemployment, for example, is federally funded, but state administered. The Department of Labor reported in December that the following states were behind in remediating their unemployment systems: Connecticut, Delaware, the District of Columbia, Hawaii, Illinois, Kansas, Louisiana, Massachusetts, Missouri, Montana, New Hampshire, New Mexico and Vermont.

In his testimony before the Committee on October 2, 1998, John Thomas Flynn, CIO of the State of California, and president of NASIRE stated that compliance among the 50 states with all aspects of mission-critical legacy systems ranged individually from under 10% complete, to more than 90% complete. According to the NASIRE survey results, just under half (24) of those responding had completed remediation of at least 50% of their mission-critical systems. Mr. Flynn noted that no state had declared itself 100% complete as yet.

Data provided by the Gartner Group indicate that only 50% of the states are evaluated as at Level III Status under the Gartner Group's scale. A Level III rating indicates that the state has completed its project plan; has assigned resources; has completed a detailed risk assessment, remediated; and has tested 20% of mission-critical systems, conducted vendor reviews and has completed contingency plans. Thirty percent of the states are listed at Level II, indicating that they at least have developed an inventory of operational dependencies. Ten percent of the states are evaluated as Level I, indicating that they have begun their projects, are aware of the problem, and have begun conducting their inventories. The remaining 10% are evaluated as "uncertain," indicating they were unaware of their Y2K preparedness status.

The GAO has advised that as of November 1998, 33 states had completed 75% of their verification of federal data exchanges. GAO found that as of June 30, 1998, approximately one half of the state disability determination systems had not been renovated, tested, and certified

Y2K compliant. Additionally, over 90% of state Medicaid, 70% of state Temporary Assistance for Needy Families and 75% of the state Food Stamp Program systems were not Y2K compliant as of August 1998 according to GAO statistics.

Survey data recently released by NACO, collected from 500 counties, indicate that only 50% of the respondents have countywide plans to address Y2K issues. Of the 16 counties with populations over 500,000, all but one have a countywide plan. Seventy-four of the 119 counties having populations below 10,000 reported that they have not prepared a Y2K plan.

Fifty-four percent of the counties surveyed reported that they have no contingency plans for Y2K disruptions. Twenty-two percent reported that they had prepared Y2K contingency plans. Fifty percent of the largest counties in the survey stated that they have contingency plans, while only 19 of 119 counties in the smallest population group (population below 10,000) had one. The 500 survey respondents reported a total cost estimate of over $283 million for Y2K compliance.

A survey published by the Office of the New York State Comptroller in September 1998 indicates that 100% of New York's counties have made preparations for Y2K. Twenty-six percent of the cities, 54% of the towns, 48% of the villages and 61% of the fire districts reported that they had not made Y2K preparations.

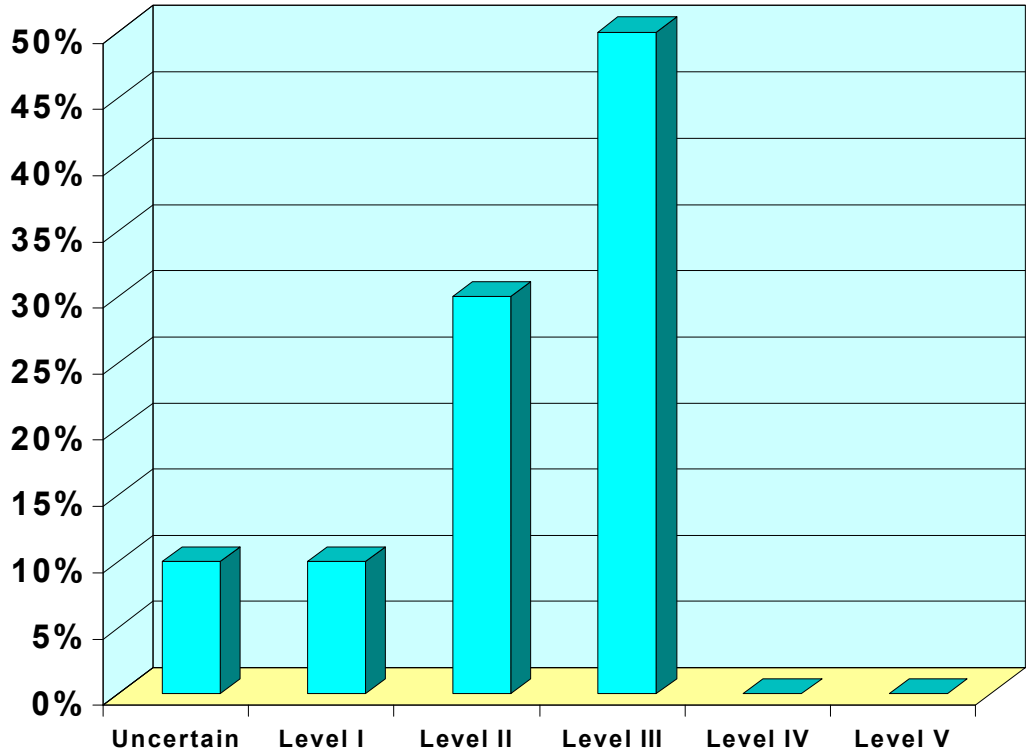
Concerns

The Committee has serious concern about the Y2K readiness of state and local governments.

This concern is supported by all of the previously cited surveys, which, when taken, together indicate a vast disparity in the readiness level of the individual states, and a disturbingly low overall level of preparedness on the part of county and local government jurisdictions.

Year 2000 Status of the 50 States*

Note: Data includes assessment of information systems owned and managed by state governments for purposes such as law enforcement, public health and education programs. It does not include private sector or county- and local-government computers or other infrastructure.



Rating is done with GartnerGroup "COMPARE" methodology. Levels of readiness are defined as:

- **Level I** - Getting started, champion identified, awareness, begin inventory
- **Level II** - Develop detailed inventory of operational dependencies
- **Level III** - Project plan completed, resources assigned, detailed risk assessment, remediate and test 20% of mission-critical systems, vendor reviews, complete contingency plans
- **Level IV** - Complete remediation and testing of remaining 80% of mission-critical systems, contingency strategies implemented for mission-critical dependencies
- **Level V** - Remaining systems and dependencies completed and policies in place to avoid non-compliant issues after compliance is reached

** Note: These data are provided courtesy of the Gartner Group, Stamford, CT.*